FEDERAL TRADE COMMISSION

I N D E X

FEDERAL TRADE COMMISSION

In the Matter of:)
REPORT TO CONGRESS PURSUANT TO)
CAN-SPAM ACT.) Matter No. P044405
---------)

WEDNESDAY
MARCH 3, 2004

Room 238
Federal Trade Commission
600 Pennsylvania Ave., N.W.
Washington, D.C. 20580

The above-entitled matter came on for conference, pursuant to agreement at 2:00 p.m.

APPEARANCES:

ON BEHALF OF THE FEDERAL TRADE COMMISSION:

DANIEL SALSBURG
COLLEEN ROBBINS
SHERYL DREXLER
MICHELLE CHUA
JULIE BUSH
Federal Trade Commission
6th Street and Pennsylvania Avenue, N.W.
Washington, D.C. 20580-0000

PARTICIPANTS (VIA TELEPHONE):

DAVID SORKIN, John Marshall Law School Professor
BEN EDELMAN, Harvard Law School Student

P R O C E E D I N G S

MR. SALSBURG: We're going to go on the record. We have a court reporter here. I think we explained that in the first e-mail we sent you.

MR. EDELMAN: Yes.

MR. SALSBURG: There are going to be a few formalities as we begin. Today is Wednesday, March 3, 2004. It's about two p.m. Eastern time, and we're meeting today with Ben Edelman and David Sorkin, who are both participating via telephone. The purpose of this meeting is to discuss a possible National Do Not E-mail Registry.

The meeting is being transcribed by a court reporter, and since you are on the telephone, she does not have the benefit of seeing you speak, so for the first few times that you talk, if you could identify who you are until she picks up the tenor of your voice, that would be very helpful.

I'm Dan Salsburg. I'm an attorney in the FTC's Division of Marketing Practices. I'm here today in Washington with Colleen Robbins and Sheryl Drexler, my colleagues. Ben and David, if you could each identify yourself and the positions and schools that you're at.

MR. EDELMAN: Sure. I'm Ben Edelman. I'm a

student at Harvard Law School, and also in the Department of Economics at Harvard University, and I write about Internet regulation.

MR. SORKIN: I'm David Sorkin. I'm a professor at the John Marshall Law School in Chicago, and I'm affiliated with the Center for Information Technology and Privacy Law.

MR. SALSBURG: As you are both aware, Section 9 of the CAN-SPAM Act directs the Commission to submit to Congress a report concerning a plan for implementing a National Do Not E-mail Registry and a timetable for implementing such a registry. The CAN-SPAM Act calls upon the FTC to evaluate whether there are any security, privacy, technical, enforceability or other concerns that the Commission may have regarding such a registry.

This report is due in Congress on June 16, which means the Commission has a very short time frame to collect information, formulate its views and prepare the report to Congress. We're in the process of collecting the information from as many sources as possible in this short amount of time, and we appreciate your willingness to talk with us and bring your perspectives to bear here.

Your statements today may be cited in this report to Congress. That's one of the purposes of our having

the court reporter here.

I thought that probably the best way that we could start was for us to lay out some possible models that a Do Not E-mail Registry could take and hear your thoughts on whether any of these models would be effective in reducing the amount of spam or whether they would pose any security or enforceability problems.

So why don't I start with the first model, but before I do that, we've been joined by Julie Bush and Michelle Chua, two of our colleagues here at the FTC. They have been asked to draft another report to Congress which concerns a possible reward system or bounty system in which members of the public would receive monetary compensation for turning in spammers.

At the end of our questions about a possible Do Not E-mail Registry, Julie is likely to be asking you some questions about a possible reward or bounty system as well.

Let's turn to the National Do Not E-mail Registry. One possible model would be similar to the model used by the Commission in the Do Not Call Registry for telemarketing. Under a similar model for Do Not E-mail, you could have consumers submit their individual e-mail addresses to the FTC, which would place them in a database. Copies of this database would be made

available to e-mail marketers who would then scrub their mailing lists, and delete from their mailing lists any e-mail addresses appearing on the registry. Do either of you have any thoughts about such a registry model?

MR. SORKIN: This is David Sorkin. I don't think that that's practical. First of all, I don't think consumers will willingly give their addresses to be included on the list, and so the participation rate is likely to be very low.

Even taking that aside, it's very likely that the list will be abused unless it's provided in a way that prevents marketers from reverse engineering it and getting a copy of the raw addresses.

MR. EDELMAN: This is Ben Edelman. The latter concern of Dr. Sorkin seems to me to be the more serious of the two. I think consumers probably could be convinced to submit their e-mail addresses to the system if there were a good reason to do so and if the system seemed sensibly designed, but I'm uncertain as to how you would go about designing a system that didn't invite abuse by the sort of disreputable junk mail senders who are sort of the people already flouting CAN-SPAM.

MR. SALSBURG: Ben Edelman, do you have any thoughts on how such a system could be made more impervious to abuse?

MR. EDELMAN: Let me offer you two possible methods. I don't mean to endorse each of these methods. I think they're flawed, but I think they're better than the base method, so to recap the base method, the base method is you receive ten million American e-mail addresses of people who don't want to get spam. You put those on a CD, and you mail copies of that CD to anyone who -- either the business is sending out e-mail and doesn't want to send e-mail to those people who have opted-out through the Do Not E-mail Registry, so that's the base case.

What's the problem there? The problem there is that if you've got copies of the CD floating around, it's a CD of folks to whom junk e-mail could be sent, and that's a bad idea that we're putting the government in the business of almost helping spammers. That's not what we want to do, so two variations that are possible alternatives here.

One, the government would provide some sort of a web based service for on demand testing by a mail transmitter as to whether or not a given e-mail address was on the list. Rather than you sending a CD of all Do Not E-mail addresses to mail transmitters, you would ask transmitters of e-mail to check each e-mail address that they were preparing to send a message to. They would

have to check each e-mail address against the central database, against the Do Not E-mail Registry, through some sort of a web based service.

You're preparing to send an e-mail to edelman@law.harvard.edu. Well, before you do that, you better go to the FTC site, submit the edelman@harvard.law.edu intending to transmit a query and receive back an answer saying either Edelman is or is not participating in the Do Not E-mail Registry.

The downsides here, one, it would provide a huge amount of information to whatever agency was operating the Do Not E-mail Registry. They would get the e-mail addresses of everyone that mail senders were considering sending e-mail to, and that might be considered unduly invasive. Then mail senders would have to provide so much information to a government agency.

Second, to the extent that folks don't intend to comply with it, they would still be able to flout that perfectly easily.

Let me offer one other alternative that I'm sure you've been thinking about, but merits precise statement, which is that you would provide different copies of the list to different licensees, so that if you were preparing to send out copies of the Do Not E-mail Registry as it stood as of some date certain, you

would add to each copy of the list some trick e-mail addresses that were in fact just waiting to see if everyone ever sent junk e-mail to them.

And if they did, the inference was that someone was using the Do Not E-mail List as a way a way to track the e-mail address to which e-mails would be sent, a technical technique used by those who maintain street mailing addresses for licensing of consumers for direct marketing purposes.

You put some junk in the mailing list, bait so to speak, and see if the bait is ever coughed up, but that too seems to me unsuccessful ultimately in that the bad actors here, the ones who are sending out junk e-mail, could just as easily ignore any of these systems, so you wouldn't actually solve the problem of spam.

MR. SALSBURG: Let me turn to the first variation that you mentioned, which was on demand testing of certain addresses. Would a spammer be able to build a subset of the database? For instance, a marketer sends in a million addresses one by one. Ultimately wouldn't they have a database that would consist of a subset of the registry?

MR. EDELMAN: Certainly it would be possible for them to do so. In their initial list of a million, they would need to have some guesses as to likely e-mail

addresses. They presumably get those from the ordinary sources that folks currently use, robots, the sort of CDs that you can buy at bazaars in Asia. I'm sure there are other ways too on the web to get spam advertising CDs, so you would come up with those million by whatever method seemed convenient, and then you would check them against the Do Not E-mail Registry.

Now, to be sure there are some tricks you might use to attempt to stop folks from doing this, for example, you might again put out some kind of a bait, although it's less clear how you would do bait in an on-demand testing environment. Also you could put limitations on the number of requests any given individual or firm could make in a given time period, but then again there are going to be some folks who want to and need to test the list for millions and millions of e-mails sent every single day because that's the business they're in.

And so if the limits were tough and tight and binding, then you wouldn't really be getting anywhere.

MR. SALSBURG: The second variation you mentioned involved delivering different copies of the list to different marketers, essentially a unique copy of the list, each one containing unique dummy addresses.

MR. EDELMAN: Exactly.

MR. SALSBURG: Would such a variation stop abuse by spammers, or simply provide the FTC with a means of determining that an abuse had occurred?

MR. EDELMAN: It would allow the FTC to determine that an abuse had occurred, but to be sure, if you add the requirement that parties licensing the list agree to some set of provisions restricting their use of the list, especially if you found out who they are or where their assets are, how it is that you would go about suing them and recovering from them if it came to that, you might be better equipped to pursue violations at that point.

MS. ROBBINS: You explained that it probably would not solve the spam problem. Why do you say that?

MR. EDELMAN: Well, background problem here. I would love to hear what Professor Sorkin thinks about this too. My own sense is that the Do Not E-mail Registry cannot solve the spam problem because the folks actually sending large amounts of spam, especially spam not in compliance with the CAN-SPAM Act, are not likely to comply with what the U.S. government tells them to do either because they're not in the United States or because they think they're doing an awfully good job of hiding who they are and where they are.

In any event, for whatever reason, they are

already outlaws, and you can see it in the sorts of goods and services that they're offering for sale. You can see it in their methods of advertising, the typos and other tricks. The people are not going to alter their behavior merely because black letter written on a piece of paper somewhere tells them to, but that's a pretty serious problem.

It's not clear what we can do about it within the realm of the sorts of methods we're discussing today, the sorts of methods that CAN-SPAM directs us to consider, but it definitely speaks to the ultimate success of any of these methods.

MR. SALSBURG: And, David Sorkin, do you see any ways to keep a model of individual e-mail addresses added to a registry list secure?

MR. SORKIN: I think basically it would have to be some kind of variation on the models that Ben suggested. My understanding is there's at least one company promoting a technology that encrypt the database of e-mail addresses presumably to do something like the web site that Ben suggested, but probably in an offline setting.

That can certainly be combined with trick or seed addresses for different clients in order to monitor whose violating the terms, but I would also echo and

maybe expand upon Ben's remarks about likely compliance on a larger scale.

There's really two groups of spammers that are of potential concern. One is the spammers who are prevalent today, most of whom are breaking state laws with little regard to even the least onerous provisions, for ones who aren't labeling ADV or forging headers and so on, and they're going to ignore whatever the FTC does.

The other group is of much more concern to me, and that's law abiding legitimate marketers, and those are the ones who are going to be paying, if need be, for access to the registry. Those are the ones who are just now starting to think of spamming, and those the ones I think we have to design the registry for.

Now, we have to design it in such a way that it doesn't make the problem worse for fraudulent spammers, which would include giving them a copy of the master Do Not E-mail Registry, but I think for the most part we need to set up a system that prevents those legitimate marketers from being able to spam everybody, even people who prefer not to receive it.

MR. SALSBURG: Let's move on to another model that people have proposed. In this model, instead of individual e-mail addresses being put on a

registry, domains such as ISPs or businesses could register their entire domain as being a spam free zone.

MR. SORKIN: This is David Sorkin again. I think that's really the only practical way to do this. It could certainly be combined with some requirement that the domain registrant or owner certify that all of the addresses within that domain have agreed, probably by standard contract, that they don't want to receive unsolicited commercial e-mail.

So, for example, AOL could in its terms of service, specify that all of its users agree that aol.com is going to be listed on the registry or that they don't want to receive unsolicited commercial e-mail, and then in fact it would be a registry of domains that appear in e-mail addresses of people who don't wish to receive e-mail.

So I think that that can certainly be done, and of course there are a lot fewer privacy and security concerns with maintaining a list of say a million domains rather than a trillion individual e-mail addresses.

MR. EDELMAN: It's less clear to me though that that would -- this is Ben Edelman, that that would solve -- I'm not sure. Something like the political aspect is the problem. I don't have a script statement

of exactly what rubs me the wrong way by opting out on that domain name by domain name basis, but I guess it basically comes down to the following: That my prediction of what would likely happen is that a bunch of the big domain names that are responsible for a huge amount of user's e-mail, Hotmail, AOL, Yahoo! Mail and so forth, they would all opt-out, and quickly where would that leave direct marketers?

It would really put them in a tough spot as far as sending out legitimate advertising messages, not that I want to jump to their defense too quickly, but it seems like you would have a difficult political problem on your hands where there would be a constituency that considered itself aggrieved and would seek to have that grievance rectified as they saw fit, such that this wouldn't be the last of the situation.

MS. ROBBINS: Do you think that there would be a way with a domain wide opt-out system that permission based or transactional e-mail could still get through? That way, legitimate marketers who are only sending out permission based e-mails would be able to still get their mail through?

MR. EDELMAN: I think certainly they would have to find a way such as do it anyway, not withstanding what the law says and see what happens after that. It

does seem like it gets to be a little bit of a mess where you're being told not to do it on one hand, but then the user has accepted it on the other hand. It's a complicated set of contingencies.

MR. SORKIN: Yeah, I think scope, the applicability of the registry would have to be somewhat narrower than most of the rest of the law. Most of CAN-SPAM applies to commercial e-mail, which excludes transactional messages, but includes messages where there's some sort of relationship.

I think the registry should apply only to unsolicited commercial e-mail, that is where there is no or no recent relationship, so that transactional messages wouldn't be an issue. Even secondary use marketing messages from a business to its own customers probably shouldn't be covered by the registry.

We may get into some circumvention issues with, for example, people promoting sweepstakes in order to gather e-mail addresses and then using them for spam, just as telemarketers are doing currently to evade the Do Not Call List, but I think that's a matter that the FTC will be in a better position to deal with in a few months.

MR. SALSBURG: Seeing how most ISPs have anti-spam policies already in place, what would an ISP

gain from putting its name on a registry?

MR. EDELMAN: The anti-spam policies that ISPs typically have already in place, my understanding is that there are basically two genres of such policies: First most ISPs prohibit their customers from sending or originating unsolicited mail. If you sign up for AOL and use your AOL account to send out 10,000 pieces of junk mail, that's bad. You shouldn't have done it. You're in breach of your sign up license agreement, and they'll terminate your service as soon as they notice and get around to it.

That's one set of policies. Two: Some ISPs take steps to attempt to protect their customers from undesired e-mail through the installation of junk mail filtering, so this falls under the second rather than the first. At least it's closer to the second rather than the first, but it doesn't seem entirely duplicative, at least to the extent that efforts of the second at junk blocking junk e-mail as it arrives have been incomplete and only partially successful at best.

I know a lot of mail gets through my filters, a lot of undesired mail, so this would be as a complement to that, an extension to that.

MR. SORKIN: I think that's true. I would take it maybe a step further and say most ISPs at least

attempt the latter as well as the former type of policy; that is, they attempt to enforce a policy that prohibits the sending of spam to their own subscribers.

The main reason why they're not able to use that as an effective tool against spam is that they generally don't have the legal power to enforce that policy against senders with whom they're not in privity. In extreme causes they can through trespass law or otherwise, but generally it's very difficult for an ISP to claim that somehow a sender has a contractual obligation to it not to send spam when otherwise the parties are strangers.

MR. SALSBURG: If a large portion of spam comes from marketers using false headers or other techniques to confuse where they're located, or it may come from abroad or through relays that are located abroad, how effective do you think a domain wide registry would be given enforcement limitations?

MR. SORKIN: I don't think we would have much effect on that kind of spam.

MR. EDELMAN: I agree.

MR. SALSBURG: So it would have an effect on I guess the so-called legitimate marketers who use spam as an advertising medium?

MR. SORKIN: Right, I think that's the only

group that almost anything in this law is likely to have much effect on.

MR. SALSBURG: Do you have any other thoughts on the domain wide registry before we move on?

MR. SORKIN: I would say that if you're going to do a registry, that's the way it ought to be done.

MR. SALSBURG: Let me move on to a third possible model. Imagine the first model that we talked about, the list of individual e-mail addresses being registered with the Commission, but instead of the Commission delivering a copy of the database to marketers, the Commission would deliver the database to a third-party forwarding service or a number of them. These would be companies or organizations that had been picked carefully by the Commission based on their security policies and their database management policies, and that when a marketer wanted to send commercial e-mail, it would submit its mailing list to the third-party.

The third-party would scrub the list, and then send along only those e-mails that were to addresses not on the registry. In other words, the marketer would never see or obtain any copy of the registry and would have no way of knowing whether any of the e-mail addresses they submitted to the third-party forwarding

service were on or off the registry.

MR. EDELMAN: Well, certainly that begins to speak to the kinds of concern I was attempting to say with my two alternatives at the start of the call. It does seem like you're just shifting the level of responsibility from the actual sender of the messages to this new genre of mail forwarding services, so the folks you have to worry about doing things that are illegal or unaccountable are the forwarding services rather than the actual senders themselves.

It seems like you're going to create some considerable additional costs in having these middle men -- additional complexity, not obvious that all of that is great. It seems like it's not desirable. On the other hand, it does at least reduce the number of folks who have to license the registry data, and that means it's not going to get out quite as readily perhaps.

MR. SORKIN: I think that's true. There's a tremendous amount of overhead here. The other thing I think we ought to be considering is what the net effect of this is going to be if the registry is a success. In the case of the Do Not Call List, we're looking at maybe half of the public bothers to get on the list. A lot of people don't receive enough telemarketing calls to bother, and a few people actually like them.

In the case of spam, I think the target participation rate ought to be well over 99 percent; that is, the registry ought to be well enough designed, secure enough, well publicized and so on, whether through ISPs or otherwise so just about everybody is on it.

So if we create a complex mechanism for forwarding commercial e-mails to those few people who aren't on the registry, we're really just talking about the people who screwed up and didn't get listed, and I think it may be impractical to set up a system for that. If there are a lot of people not on the registry, then I think we have a failure somewhere else in the system.

MS. ROBBINS: Then do either of you have a sense of how many e-mail addresses might be registered if 99 percent of the people might register?

MR. SORKIN: I would say it's probably in the trillions. Many people have very large numbers of e-mail addresses. If you can register an e-mail address containing a wild card, for example, an individual who holds a domain name, for example, might want to register every e-mail address where the user name starts with the letters A through M and include addresses at thousands of different sub domains within the domain

name.

So the total, if you're talking about individual e-mail addresses, is going to be extremely high.

MR. EDELMAN: Certainly if you don't allow domain name based wild card systems, it's going to be particularly high. If we put that aside and we put aside the folks like I'm sure myself, like Professor Sorkin, who has hundreds or thousands or truly infinitely many different e-mail address on which in principle we could receive messages.

If we talk about legitimate -- legitimate is not the right word, actual, individual, ordinary e-mail accounts, I think a number like a trillion is on the right border of magnitude. It's more than a hundred million and less than ten trillion, so we have it in terms of powers of ten. It's a big number.

MR. SALSBURG: Do you have any sense of how many e-mail accounts the typical consumer would have?

MR. EDELMAN: Someone is likely to have between -- what's the limiting case? The limiting case is like a half to a third. My mother and father share an e-mail account, okay? That's not true anymore, but it used to be. That would be the lower bound.

Now, on the upper bound, I have a home account. I have a work account. I have an account that my

college or university gave me when I graduated for the rest of my life, and I have a free Yahoo! account that I made a few years back, so we're up to like, what, five to six per person at that point. That seems to me perfectly realistic.

MR. SORKIN: I think that's true, and of course some ISPs will provide multiple e-mail addresses within a particular account.

MS. DREXLER: How likely is it that the average person would actually register all those different wild card possibilities?

MR. SORKIN: Well, I'm not sure, but certainly the experience with the Do Not Call List was that the system was set up so people could register more than one phone number, and it certainly seems likely that more people have multiple e-mail addresses than have multiple phone numbers, especially in the case of phone numbers where supposedly it's limited to residential numbers.

MR. EDELMAN: I think the analogy to the Do Not Call List breaks down pretty quickly here because for phone numbers you're paying somebody to have a phone number. The better analogy would actually be to individual extensions on a PBX because I'm putting aside that Do Not Call was about home phones rather than business phones.

The issue is that some individuals register their own domain names, at which point they could have arbitrarily many e-mail addresses behind a single domain name, just as there could be arbitrarily many extensions behind a single PBX phone number, so where does that leave you?

I guess in a system that was based on individual e-mail addresses rather than domain names, you might still want to allow wild cards, at least to the extent that an individual had personally register a domain name rather than an ISP registering a domain name, but that seems administratively, excessively complicated and infeasible so you wouldn't really want to go down that path.

MR. SORKIN: Right, and that's why I suggested that the registrants, perhaps the domain registrants or whoever submits the address as part of the submission might need to certify that anyone who receives e-mail that matches the wild card or the domain have authorized the inclusion of the address in the list.

MS. ROBBINS: Before we move on, I just want to ask: Do either of you see any difference in trying to enforce or the enforceability for any of these three models in terms of tracing and identifying the spammers?

MR. SORKIN: I don't think so. I suppose the

middle one is likely to be more transparent because the list can be freely published, so that may aid some in enforcement, but I don't think it matters much.

MR. EDELMAN: Again, the only enforcement issue that jumps out at me is that if you implemented this in a way that allowed tracking of what bad actor had obtained the whole list and was using it as a list of addresses to send messages to, you might find that through the dummy records we discussed, but putting that aside they all seemed equally flawed in enforcement, but no one better than the other.

MR. SALSBURG: Well, let's move on to another possible registry model, and this would be a registry that was not of e-mail addresses nor was it of domains. Instead it would be a registry of authenticated e-mail marketers.

Under this approach, an e-mail marketer would be required to register with the Commission. They would obtain a registration number, which would be required to be included in the headers of any commercial e-mail they sent. They would also be required to register the IP addresses and the domain names from which they sent their outgoing commercial e-mail.

ISPs and other domain owners would be provided access to the database of registration numbers,

corresponding IP addresses and domain names and could adjust their filters. If there was a match of a registration number and sending IP address, they would know that it was an authenticated e-mailer. And if there was no match, they would know it was somebody who was trying to hide their identity.

MR. SORKIN: I think that would be valuable if the point is for recipients to be able to block anything that comes from an authenticated e-mailer. Of course then you want to limit it to unsolicited rather than all commercial because there's a lot that you would want to get through that wouldn't be commercial that wouldn't be subject to that system, but I gather that's not the point.

MR. EDELMAN: I think these kinds of systems where there are databases of which mail servers ought to be sending messages to which users with which kind of header data, this method of building an e-mail security system is the right approach, and it is the approach that now seems to be most likely to take hold and actually solve this problem, but I think you're right to wonder whether there is some way to use similar methods here as to a Do Not E-mail Registry or a registry of legitimate transmitters.

What I would think you would want to do, if you

were to proceed in this way, is look very closely at the specification I guess it's called SPF, S like Sam, P like Peter, F like Frank, which is the method proposed by Internet engineers for authenticating messages as legitimately and authoritatively and with the authorization of a domain name registrant coming from official e-mail users of that domain name.

If you were able to add some sort of a tag to an SPF record that said, "And not only did they come from this domain name but this domain name is associated with a bona fide FTC registered mail transmitter," that would actually be helpful in informing the filter that this was good stuff.

On the other hand, the mere presence of a legitimate SPF header that checked out when you do the cross references was itself to be taken as favorable data by the mail filter that looks at SPF headers, and so it seems to me that maybe this kind of approach would actually be superfluous given what the engineers are already talking about doing.

MR. SORKIN: There's a couple other concerns I want to raise. One is that generally the experience we've had with trying to hard code technology into the law has not been successful. The law can't change quickly enough. It may stifle the development of

technology, and frequently we just get the technology wrong when we try to put it into the law.

The other problem is really related to the point I made before, that we need to examine what kind of mail we're talking about authenticating. If we're talking about commercial e-mail that is subject to the CAN-SPAM Act, most of it is stuff that we would want to be able to enable people not to get, and so the likely effect of such an authentication system is that recipients and Internet providers will recognize e-mail as it comes in authenticated and automatically block or delete all of that mail because so much of it is spam, at least if spam is included in that set.

MR. SALSBURG: Why don't you expound upon that a bit. If I were an ISP, am I more or less likely to block e-mail if it's properly authenticated?

MR. SORKIN: Well, it strikes me sort of similar to an ADV label. Most spammers don't put it on there, but if they did, ISPs would just delete it automatically, which is probably why they don't. Authenticating e-mail is roughly the same kind of concept.

The injury caused by spam isn't the fact that we're not sure where it came from. It's the fact that it's spam that is unsolicited, bulk and usually

commercial e-mail and putting an identifier on it that tells us it's more likely that something is spam isn't going to encourage us to let it through.

MR. SALSBURG: Suppose that all commercial e-mail had to be authenticated. Would an ISP respond by blocking e-mail that had a matching registration number and IP address or would they block only those that didn't have a match and subject what didn't have a match to its other filtering technologies?

MR. SORKIN: I don't think they would do either one. The spam from legitimate marketers would be coming through authenticated, but they couldn't block that because of transactional and relationship and solicited commercial messages coming through that channel, and all the fraudulent spam would be coming through the other channel, and they couldn't block anything that wasn't authenticated because there would also be a lot of legitimate non-commercial traffic there, so I don't think it gets us anywhere.

MR. SALSBURG: Do either of you have any other thoughts on possible registry models?

MR. SORKIN: I'll throw one out. It's not fully developed. It's really a variant domain wide opt-out, listing domains on the registry. If instead of indicating that all addresses in a domain were

forbidden, if listing a domain on the registry there meant that the domain name registrant maintains its own metropolitan Do Not E-mail List, for example, if aol.com appears on the registry, that means the sender has to go to a web interface provided by AOL to check whether each address is permissible, then that gives us I think the benefits of individual choice with some control at the federal level, but doesn't require the federal government to maintain the entire database.

Of course, AOL could probably still maintain its system in such a way that the response for each individual query is there's always this person is listed on the Do Not E-mail Registry because we require all subscribers to do that, but that would at least make it somewhat more palatable to those who say that you shouldn't be able to do blanket opt-out for an entire domain.

MS. ROBBINS: Do you think that would be more difficult for the smaller ISPs? Or, do you think there would be no difference between AOL doing it as opposed to some local ISP?

MR. SORKIN: It probably would be fairly simple because the ISP could simply say the URL. Maybe the registry would -- say if it's a domain name, it would give a URL where the registry for that domain can be

reached, and the smaller ISP perhaps at a threshold might be able to post a page saying, "This ISP has fewer than a hundred users, all of whom are in the Do Not E-mail Registry."

So possibly with a threshold or some other capacity, it shouldn't be too difficult. I think just about every ISP has the capacity to maintain a web page. I think that's really all that's got to be required.

MS. ROBBINS: Do you think it should be the government requiring that each ISP must maintain this kind of list, or would it be the choice of each individual ISP?

MR. SORKIN: I think it's got to be a matter of contract and really subject to state laws. If a state wants to give individual Internet subscribers the right to be in the opt-out list and without having to change their e-mail addresses, then that obviously creates a problem for ISPs subject to that law. I doubt that would happen, but I don't know see how it can't be resolved by contract between the contractor and the ISP.

MR. SALSBURG: Under this model, there would be no role for federal enforcement of violations of such a list?

MR. SORKIN: Oh, no. The federal government

still has an enforcement role. They might have to get some certification from the Internet provider that in fact the address was opted-out. Also it could be that AOL would respond by saying, "If you don't want to be on our opt-out list, you need to change your e-mail address to aolspammers.com" or something like that instead of an entirely different domain name for which, of course, they would probably charge a much higher monthly fee to reduce traffic, but I think that can be left to individual ISPs to figure out how they're going to comply with that.

MR. SALSBURG: If this model enables an individual consumer to have more choice than a domain wide registry where domains were registered with the FTC, would -- I'm sorry?

MR. SORKIN: Go ahead. I thought you were done.

MR. SALSBURG: No, that's okay. If that were the case, that there was individual choice, so as an AOL subscriber I could inform AOL I wanted to get spam and an e-mail marketer could query AOL to find that out, is there any change in the security concerns between the database being housed by AOL or another ISP or by the federal government?

MR. SORKIN: I don't think there's much of a

security concern for releasing addresses of people that want to receive spam because they're already getting that. I suppose they might get more if the ISP gave out their addresses, but they wouldn't have to do that. They could certainly give a false answer. I don't know if anyone has tried to check an address anyway to disguise those, so I don't think it's vulnerable to dictionary attack.

But first whether this gives really more consumer choice, I think it probably doesn't because so few ISPs are really going to give people a realistic option to keep receiving spam when it's not truly in the consumer's interest, and it's certainly not in the ISPs interest to do that, but AOL may set up a separate domain for people that really want spam, but nobody is really going to use that.

MR. EDELMAN: To jump in here, I guess I want to go back to the first question of: Does any of this work? Would this be worth talking about if Congress hadn't told us in Section 9 that we had to talk about it? Unfortunately I guess I'm almost always a pessimist on most things, but I'm a particular pessimist as to solving the spam problem generally, via legal solutions and particularly with a Do Not E-mail Registry.

If I were drafting this, at least with the

information and with the analysis I have and have thought about today, I would have to tell Congress that there's nothing that can be done in the family of a Do Not E-mail Registry that seems like it's going to make things enough better to be worth the costs that are imposed on legitimate advertisers and on FTC staff who get distracted from the other important things they're supposed to be doing and Internet companies and the rest. It just isn't how you solve the problem. We've looked into it and that has to be the end of it. Now, that's going to be my bottom line of course.

As to the rest of it, I think what Professor Sorkin is saying is exactly right. We're going in the right direction but realistically we don't have to talk about folks opting-in to get a lot of spam. That just isn't the problem we're trying to solve here.

MR. SORKIN: I would have to agree. I don't think this is going to do anything to solve the spam problem we have today, the fraudulent and offensive spam, the non-law abiding spammers.

MR. EDELMAN: That's exactly what we're trying to solve.

MR. SORKIN: I'm not so sure. I think we also need to be concerned about the spammers of tomorrow, the legitimate marketer today who maybe are innocently

buying list of consumers they think are opt-in and are toying with the idea of sending out mail blasts, but under CAN-SPAM, it's pretty clear they've got a right to do that, and if the Do Not E-mail Registry stops them, then I think it has some value.

MR. SALSBURG: Well, thank you both for taking the time to talk to us about a possible Do Not E-mail Registry. Do either of you know of anyone else you think we should talk to who might be able to offer some unique insights?

MR. EDELMAN: I thought about that at some length when you first wrote to me actually because I didn't think I could be of particular assistance to you, and certainly I didn't want to give you the bottom line I just gave you if I could think of anything that would be more helpful to you and to the folks actually getting junk e-mail rather than, "Sorry, we can't solve your problem."

I don't really know anyone who has done work in the family of Do Not E-mail Registry that leads to the conclusion that by implementing it according to method X, you can solve the problem all together. Maybe Professor Sorkin has written more in the field and has more to say.

MR. SORKIN: One person you've probably had

contact with already is Matthew Prince of "Unspam," who is pushing a technology that would do some sort of encrypted address registry. I'm not sure how much he has to say on the policy side, although I think he's definitely worth talking to as well.

MR. SALSBURG: Thank you. We're going to turn this over now to Michelle Chua and Julie Bush who are going to talk with you about the possible reward system, the bounty system under the CAN-SPAM Act. Thank you both again, and if you have any further thoughts on this, you should feel free to send us an e-mail or give us a call.

MR. SORKIN: I have one question. You said there was a transcript being taken. Is that going to be made available to us?

MR. SALSBURG: That's a good question. I'll get back to you on that.

(Discussion off the record.)

C E R T I F I C A T I O N O F R E P O R T E R

MATTER NUMBER: P044405
CASE TITLE: INTERVIEWS IN CAN-SPAM REPORT TO CONGRESS
HEARING DATE: MARCH 3, 2004

I HEREBY CERTIFY that the transcript contained herein is a full and accurate transcript of the tapes transcribed by me on the above cause before the FEDERAL TRADE COMMISSION to the best of my knowledge and belief.

DATED: MARCH 10, 2004

DEBRA L. MAHEUX

C E R T I F I C A T I O N O F P R O O F R E A D E R

I HEREBY CERTIFY that I proofread the transcript for accuracy in spelling, hyphenation, punctuation and format.

DIANE QUADE